J. Math. Kyoto Univ. (JMKYAZ)
39-2 (1999) 233–248

Generating elements for B_{dR}^{+}

By

Adrian Iovita and Alexandru Zaharescu

Introduction

Let us fix a prime number p. Then B_{dR}^{+} denotes the ring of p-adic periods of algebraic varieties defined over local (p-adic) fields as considered by J.-M. Fontaine in [Fo]. It is a topological local ring with residue field $\mathbf{C}_p$ (see the section Notations) and it is endowed with a canonical, continuous action of $G := \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$, where $\bar{\mathbf{Q}}_p$ is the algebraic closure of $\mathbf{Q}_p$ in $\mathbf{C}_p$. Let us denote by I its maximal ideal and $B_n := B_{dR}^{+}/I^n$. Then B_{dR}^{+} (and B_n for each $n \geq 1$) is canonically a $\bar{\mathbf{Q}}_p$-algebra and moreover $\bar{\mathbf{Q}}_p$ is dense in B_{dR}^{+} (and in each B_n respectively) if we consider the "canonical topology" on B_{dR}^{+} which is finer than the I-adic topology.

Let now L be any algebraic extension of $\mathbf{Q}_p$ contained in $\bar{\mathbf{Q}}_p$ and $G_L := \mathrm{Gal}(\bar{\mathbf{Q}}_p/L)$. In [I-Z], the authors described all the algebraic extensions of $K := \mathbf{Q}_p^{ur}$ such that L is dense in $(B_n)^{G_L}$ for some n or in $(B_{dR}^{+})^{G_L}$. Let us formulate this problem in a different way. For two commutative topological rings $A \subset B$, a subset $M \subset B$ will be called a "generating set" if $A[M]$ is dense in B.

Definition 0.1. Let $A \subset B$ be commutative topological rings, then we define "the generating degree", $gdeg(B/A) \in \mathbf{N} \cup \infty$ to be

$$gdeg(B/A) := \min\{|M|, \text{ where } M \text{ is a generating set of } B/A\}$$

where $|M|$ denotes the number of elements of M if M is finite and ∞ if M is not finite.

Then the problem *Is L dense in $(B_{dR}^{+})^{G_L}$?* can be formulated as *Is $gdeg((B_{dR}^{+})^{G_L}/L)$ zero?* For example Theorem 0.1 of [I-Z] can be restated as:

Theorem 0.1. *If L is not a deeply ramified extension of K then*

$$gdeg((B_n)^{G_L}/L) = 0 \quad \text{for all } n \quad \text{and} \quad gdeg(B_{dR}^{+})^{G_L}/L) = 0.$$

A characterization of deeply ramified extensions L of K satisfying $gdeg((B_{dR}^{+})^{G_L}/L) = 0$ is obtained in [I-Z], Theorem 0.2. As not all deeply ramified extensions of K have this nice property, [I-Z] left open the problem of describing $(B_n)^{G_L}$ for all n and $(B_{dR}^{+})^{G_L}$, for a general deeply ramified extension L. The first part of this paper (section 2) supplies such a description, namely we prove

Communicated by Prof. K. Ueno, November 25, 1997
Revised September 22, 1998

Theorem 0.2. *If L is a deeply ramified extension of K then*

i) *there exists a uniformizer z of B^+_{dR} (i.e. a generator of I) such that $z \in (B^+_{dR})^{G_L}$*

ii) *$L[z]$ is dense in $(B^+_{dR})^{G_L}$, and if we denote by z_n the image of z in B_n, then $L[z_n]$ is dense in $(B_n)^{G_L}$ for all n.*

In other words, Theorem 0.2 tells us that if L is deeply ramified then $gdeg((B_n)^{G_L}/L) \leq 1$ for all n and $gdeg((B^+_{dR})^{G_L}/L) \leq 1$.

The second part of the paper (sections 3 and 4) is concerned with a problem of a different nature. It is known ([I-Z]) that B_n is a Banach algebra over $\mathbf{Q}_p$ for all n. We are interested in constructing a "nice" integral, orthonormal basis of B_n, as a Banach space over $\mathbf{Q}_p$. First we prove a surprising fact, namely that B^+_{dR} is the completion of the polynomial ring in one variable over $\mathbf{Q}_p$ in a suitable topology, i.e. we prove the following

Theorem 0.3. $gdeg(B^+_{dR}/\mathbf{Q}_p) = 1$.

Theorem 0.3 provides us with an element $Z \in B^+_{dR}$ such that $\mathbf{Q}_p[Z]$ is dense in B^+_{dR}. We can use this "generating" element Z to construct an orthonormal basis for B_n over $\mathbf{Q}_p$. Namely, let us fix an $n \geq 2$ and let us denote by z the image of Z in B_n. Then we construct a sequence of polynomials $\{M_m(X)\}_{m\geq 0}$ in $\mathbf{Q}_p[X]$, with the property that $M_0(X) = 1$ and $\deg(M_m(X)) = m$ for all m, such that

Theorem 0.4. *The family $\{M_m(z)\}_m$ is an integral, orthonormal basis of B_n over $\mathbf{Q}_p$, i.e.*

i) *For any $y \in B_n$ there exists a unique sequence $\{c_m\}_m$ in $\mathbf{Q}_p$ such that $c_m \xrightarrow{v} 0$ and $y = \sum_m c_m M_m(z)$.*

ii) *For y and $\{c_m\}_m$ as in* i) *above we have*

$$w_n(y) = \min_m v(c_m)$$

where let us recall that w_n is the valuation which gives the Banach-space norm on B_n.

iii) *For y and $\{c_m\}_m$ as in* i) *above, we have: $w_n(y) \geq 0$ if and only if $c_m \in \mathbf{Z}_p$ for all m.*

We end the paper (section 5) with some examples and problems concerning metric invariants for elements in B^+_{dR}.

Notations. Let p be a prime number, $K = \mathbf{Q}_p^{ur}$ the maximal unramified extension of $\mathbf{Q}_p, \bar{K}$ a fixed algebraic closure of K and $\mathbf{C}_p$ the completion of $\bar{K}$ with respect to the unique extension v of the p-adic valuation on $\mathbf{Q}_p$ (normalized such that $v(p) = 1$). All the algebraic extensions of K considered in this paper will be contained in $\bar{K}$. Let L be such an algebraic extension. We denote by $G_L := \mathrm{Gal}(\bar{K}/L)$, $\hat{L}$ the (topological) closure of L in $\mathbf{C}_p$, $\mathcal{O}_L$ the ring of integers in L and m_L its maximal ideal. If $K \subset L \subset F \subset \bar{K}$, and F is a finite extension of L, $\Delta_{F/L}$ denotes the different of F over L.

If A and B are commutative rings and $\phi : A \to B$ is a ring homomorphism we denote by $\Omega_{B/A}$ the B-module of Kähler differentials of B over A, and $d : B \to \Omega_{B/A}$ the structural derivation.

Let $\mathscr{A}$ be a Banach space whose norm is given by the valuation w and suppose that the sequence $\{a_m\}$ converges in $\mathscr{A}$ to some α. We will write this: $a_m \xrightarrow{w} \alpha$.

If A is a subring of the commutative ring B and $M \subset B$ is a subset, then we denote by $A[M]$ the smallest A-subalgebra of B which contains M.

1. Some constructions, definitions and results

We'd like to first of all recall some of the main results and definitions from [Fo], [F-C] and [I-Z], which will be used in the paper. We'll first recall the construction of B_{dR}^+, which is due to J.-M. Fontaine in [Fo]. Let R denote the set of sequences $x = (x^{(n)})_{n\geq 0}$ of elements of $\mathcal{O}_{C_p}$ which verify the relation $(x^{(n+1)})^p = x^{(n)}$. Let's define: $v_R(x) := v(x^{(0)})$, $x + y = s$ where $s^{(n)} = \lim_{n\to\infty}(x^{(n+m)} + y^{(n+m)})^{p^m}$ and $xy = t$ where $t^{(n)} = x^{(n)}y^{(n)}$. With these operations R becomes a perfect ring of characteristic p on which v_R is a valuation. R is complete with respect to v_R. Let $W(R)$ be the ring of Witt vectors with coefficients in R and if $x \in R$ we denote by $[x]$ its Teichmüller representative in $W(R)$. Denote by θ the homomorphism $\theta : W(R) \to \mathcal{O}_{C_p}$ which sends $(x_0, x_1, \ldots, x_n, \ldots)$ to $\sum_{n=0}^{\infty} p^n x_n^{(n)}$. Then θ is surjective and its kernel is principal. Let also θ denote the map $W(R)[p^{-1}] \to \mathbf{C}_p$. We denote $B_{dR}^+ := \lim_{\leftarrow} W(R)[p^{-1}]/(\mathrm{Ker}(\theta))^n$. Then θ extends to a continuous, surjective ring homomorphism $\theta = \theta_{dR} : B_{dR}^+ \to \mathbf{C}_p$ and we denote $I := \mathrm{Ker}(\theta_{dR})$ and $I_+ := I \cap W(R)$. Let $\varepsilon = (\varepsilon^{(n)})_{n\geq 0}$ be an element of R, where $\varepsilon^{(n)}$ is a primitive p^n-th root of unity such that $\varepsilon^{(0)} = 1$ and $\varepsilon^{(1)} \neq 1$. Then the power series

$$\sum_{n=1}^{\infty}(-1)^{n-1}([\varepsilon] - 1)^n/n$$

converges in B_{dR}^+, and its sum is denoted by $t := \log[\varepsilon]$. It is proved in [Fo] that t is a generator of the ideal I, and as $G_K := \mathrm{Gal}(\bar{K}/K)$ acts on t by multiplication with the cyclotomic character, we have $I^n/I^{n+1} \cong \mathbf{C}_p(n)$, where the isomorphism is $\mathbf{C}_p$-linear and G_K-equivariant. Therefore for each integer $n \geq 2$, if we denote by $B_n := B_{dR}^+/I^n$ we have an exact sequence of G_K-equivariant homomorphisms

$$0 \to J_{n+1} \to B_{n+1} \xrightarrow{\phi_n} B_n \to 0$$

where $J_{n+1} \cong I^n/I^{n+1} \cong \mathbf{C}_p(n)$. This exact sequence will be called "the fundamental exact sequence". We denote by $\theta_n : B_{dR}^+ \to B_n := B_{dR}^+/I^n$ and by $\eta_n : B_n \to \mathbf{C}_p$ the canonical projections induced by θ.

Let us now review P. Colmez's differential calculus with algebraic numbers as in the Appendix of [F-C]. We should point out that as our K is unramified over $\mathbf{Q}_p$ and so $W(R)$ is canonically an $\mathcal{O}_K$ as well as an $\mathcal{O}_{\bar{K}}$-algebra, we'll work with $W(R)$ instead of A_{inf}. For each nonnegative integer k, we set $A_{inf}^k := W(R)/I_+^{k+1}$. We define recurrently the sequences of subrings $\mathcal{O}_{\bar{K}}^{(k)}$ of $\mathcal{O}_{\bar{K}}$ and of $\mathcal{O}_{\bar{K}}$-modules $\Omega^{(k)}$

setting: $\mathcal{O}_{\bar{K}}^{(0)} = \mathcal{O}_{\bar{K}}$ and if $k \geq 1$ $\Omega^{(k)} := \mathcal{O}_{\bar{K}} \otimes_{\mathcal{O}_{\bar{K}}^{(k-1)}} \Omega^1_{\mathcal{O}_{\bar{K}}^{(k-1)}/\mathcal{O}_K}$ and $\mathcal{O}_{\bar{K}}^{(k)}$ is the kernel of the canonical derivation $d^{(k)} : \mathcal{O}_{\bar{K}}^{(k-1)} \to \Omega^{(k)}$. Then we have

Theorem 1.1 (Colmez, Appendice of [F-C], Théorème 1). (i) *If $k \in \mathbf{N}$, then $\mathcal{O}_{\bar{K}}^{(k)} = \bar{K} \cap (W(R) + I^{k+1})$ and for all $n \in \mathbf{N}$ the inclusion of $\mathcal{O}_{\bar{K}}^{(k)}$ in $W(R) + I^{k+1}$ induces an isomorphism*

$$A_{inf}^k / p^n A_{inf}^k \cong \mathcal{O}_{\bar{K}}^{(k)} / p^n \mathcal{O}_{\bar{K}}^{(k)}.$$

(ii) *If $k \geq 1$, then $d^{(k)}$ is surjective and $\Omega^{(k)} \cong (\bar{K}/\mathbf{a}^k)(k)$, where $\mathbf{a}$ is the fractional ideal of $\bar{K}$ whose inverse is the ideal generated by $\varepsilon^{(1)} - 1$ (recall $\varepsilon^{(1)}$ is a fixed primitive p-th root of unity.)*

Some consequences of this theorem are gathered in the following

Corollary 1.1. (i) *$A_{inf}^{(n)} \cong \varprojlim (\mathcal{O}_{\bar{K}}^{(n)} / p^i \mathcal{O}_{\bar{K}}^{(n)})$ and $A_{inf}^{(n)} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \cong B_{n+1}$ for all $n \geq 0$.*

(ii) *$\Omega^{(n)}$ is a p-divisible and a p-torsion $\mathcal{O}_{\bar{K}}$-module.*

The authors have defined in [I-Z] a sequence $\{w_n\}_n$, of valuations on $\bar{K}$. We'll recall the definition and their main properties. For each $n \geq 1$ let $\mathcal{O}_{\bar{K}}^{(n)}$ be the subring of $\mathcal{O}_{\bar{K}}$ defined above. For $a \in \bar{K}^*$ we define

$$w_n(a) := \max\{m \in \mathbf{Z} \mid a \in p^m \mathcal{O}_{\bar{K}}^{(n-1)}\}.$$

Properties of w_n

a) $w_n(a+b) \geq \min(w_n(a), w_n(b))$ and if $w_n(a) \neq w_n(b)$ then we have equality, for all, $a, b \in \bar{K}$.

b) $w_n(ab) \geq w_n(a) + w_n(b)$ for all a, b.

c) $w_n(a) = \infty$ if and only if $a = 0$.

d) $v(a) \geq w_{n-1}(a) \geq w_n(a)$ for all $a \in \bar{K}$ and $n \geq 2$

e) For each $n \geq 1$ the completion of $\bar{K}$ with respect to w_n is canonically isomorphic to B_n.

f) For each $n \geq 1$, $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and $a \in \bar{K}$ we have $w_n(\sigma(a)) = w_n(a)$.

Remark 1.1. If we define the norm $\|a\|_n := p^{-w_n(a)}$ for all $a \in \bar{K}$, then w_n and $\|\cdot\|_n$ extend naturally to B_n which becomes a Banach algebra over $\hat{K}$. Furthermore the canonical maps $\phi_n : B_{n+1} \to B_n$ are continuous Banach algebra homomorphisms of norm 1. As mentioned before, $B_{dR}^+ = \lim_{\leftarrow} B_n$, with transition maps the ϕ's. The canonical topology on B_{dR}^+ is the projective limit topology, with topology on each B_n induced by w_n.

Let us now recall the concept of *deeply ramified* extension. Let $\mathbf{Q}_p \subset L \subset \bar{K}$. Then we have

Theorem 1.2 (Coates-Greenberg, [C-G]). *The following conditions on L are equivalent*

i) *L does not have a finite conductor (i.e. L is not fixed by any of the ramification subgroups of* $\mathrm{Gal}(\bar{K}/\mathbf{Q}_p)$.*)*

ii) *The set* $\{v(\Delta_{F/\mathbf{Q}_p}) \mid \mathbf{Q}_p \subset F \subset L$ *and* $[F:\mathbf{Q}_p] < \infty\}_F$ *is unbounded*

iii) *For every L' finite extension of L, we have* $m_L \subset \mathrm{Tr}_{L'/L}(m_{L'})$.

Remark 1.2. There are more equivalent conditions in [C-G], but we will not use them here.

Definition 1.1 (Coates-Greenberg, [C-G]). We say that L is a deeply ramified extension of $\mathbf{Q}_p$ if it satisfies the equivalent conditions of the above Theorem.

We'd like now to recall another result of [I-Z], which will be used in the proof of Theorem 2.2. For each $n \geq 1$ we have defined a derivation

$$d_n : \mathcal{O}_{\bar{K}}^{(n-1)} \to \Omega^{(n)}.$$

The following facts are proven in [I-Z], section 5:

1) d_n is continuous with respect to w_{n+1} on the domain and the discrete topology on the target. Therefore it extends to an $\mathcal{O}_K$-linear map from the topological closure of $\mathcal{O}_{\bar{K}}^{(n-1)}$ in B_{n+1}, which will be denoted by A_{n+1}, so $d_n : A_{n+1} \to \Omega^{(n)}$.

2) $J_{n+1} \subset A_{n+1}$, where J_{n+1} was defined before. So, by restriction we get an $\mathcal{O}_K$-linear map $d_n : J_{n+1} \to \Omega^{(n)}$, which turns out to be surjective for all $n \geq 1$.

3) Both J_{n+1} and $\Omega^{(n)}$ have canonical structures of $\mathcal{O}_{\mathbf{C}_p}[G]$-modules and d_n is $\mathcal{O}_{\mathbf{C}_p}[G]$-semilinear (let us recall that $G := \mathrm{Gal}(\bar{K}/\mathbf{Q}_p)$.)

4) Let L be a deeply ramified extension of $\mathbf{Q}_p$ and $G_L : \mathrm{Gal}(\bar{K}/L)$. Then the restriction

$$d_n : J_{n+1}^{G_L} \to (\Omega^{(n)})^{G_L}$$

is "almost surjective", i.e. the cokernel of the map is annihilated by m_L.

Finally, we'd like to recall the notion of "generating set" and "generating degree" defined in the Introduction. For two commutative topological rings $A \subset B$, a subset $M \subset B$ will be called a "generating set" if $A[M]$ is dense in B, where $A[M]$ is defined in the section Notations.

Definition 1.2. Let $A \subset B$ be commutative topological rings, then we define "the generating degree", $gdeg(B/A) \in \mathbf{N} \cup \infty$ to be

$$gdeg(B/A) := \min\{|M|, \text{ where } M \text{ is a generating set of } B/A\}$$

where we denote by $|M|$ the number of elements of M if M is finite and ∞ if M is not finite.

We have the very simple properties:

a) If $A \subset B \subset C$ then

i) $gdeg(C/A) \leq gdeg(B/A) + gdeg(C/B)$

ii) $gdeg(C/A) \geq gdeg(C/B)$.

Remark 1.3. It is not true though that $gdeg(C/A) \geq gdeg(B/A)$. For example $gdeg(\bar{\mathbf{Q}}_p/\mathbf{Q}_p) = \infty$ while $gdeg(B_{dR}^+/\mathbf{Q}_p) = 1$ (as will be shown in Theorem 3.1).

b) $gdeg(B/A)$ is invariant with respect to isomorphisms of topological rings.

c) If $A \subset B$ is a finite separable extension of fields, then $gdeg(B/A) \leq 1$.

d) If $L/\mathbf{Q}_p$ is a finite field extension, then $gdeg(\mathcal{O}_L/\mathbf{Z}_p) \leq 1$.

e) $gdeg(\mathcal{O}_{\mathbf{C}_p}/\mathbf{Z}_p) = \infty$.

Remark 1.4. In connection with e) above note that since $gdeg(\mathbf{Q}_p/\mathbf{Z}_p) = 1$ from i) above and the level 1 case of Theorem 3.1 below it follows that $gdeg(\mathbf{C}_p/\mathbf{Z}_p) \leq 2$.

2. Galois invariants of B_{dR}^+

Let L be an algebraic extension of K. Then we can state and prove the following description of $(B_n)^{G_L}$ for all $n \geq 1$ and of $(B_{dR}^+)^{G_L}$.

Theorem 2.1. *If L is not deeply ramified then L is dense in $(B_n)^{G_L}$ for all $n \geq 1$ and in $(B_{dR}^+)^{G_L}$.*

This was proved in [I-Z].

Remark 2.1. In [I-Z] the authors prove much more, namely that $(B_n)^{G_L} = \hat{L}$ for all $n \geq 2$ and $(B_{dR}^+)^{G_L} = \hat{L}$. Also, the valuations w_n restricted to L are all equivalent and they are equivalent to the usual p-adic valuation v.

Theorem 2.2. *If L is deeply ramified then*

i) *there exists a uniformizer z of B_{dR}^+ (let us recall that this is a generator of the ideal I), such that $z \in (B_{dR}^+)^{G_L}$.*

ii) *$L[\theta_n(z)]$ is dense in $(B_n)^{G_L}$ for all $n \geq 2$ and $L[z]$ is dense in $(B_{dR}^+)^{G_L}$, where z is like in* i).

Proof. i) was proved in [I-Z], but we will sketch the proof here as well. It is enough to prove that for each $n \geq 2$ there exists a uniformizer $z_n \in (B_n)^{G_L}$ such that the z_n's are compatible (i.e. $\phi_n(z_{n+1}) = z_n$). We'll prove this by induction on n. For $n = 2$ the statement follows from the fact that $(\mathbf{C}_p(1))^{G_L} \neq 0$ ([I-Z] Proposition 3.1). Let us now suppose that the statement is true for n and let us prove it for $n+1$. Let z_n be a uniformizer of B_n, invariant under G_L and let y be any uniformizer of B_{n+1} such that $\phi_n(y) = z_n$. Let us recall the "fundamental exact sequence"

$$0 \longrightarrow J_{n+1} \longrightarrow B_{n+1} \xrightarrow{\phi_n} B_n \longrightarrow 0.$$

On the one hand, $J_{n+1} \cong I^n/I^{n+1}$ is a one dimensional $\mathbf{C}_p$-vector space generated by y^n. On the other hand, as z_n is invariant under G_L, for each $\sigma \in G_L$ we have $\sigma(y) - y \in J_{n+1}$. Therefore for each $\sigma \in G_L$ there exists a unique $\zeta(\sigma) \in \mathbf{C}_p$ such that

$$\sigma(y) - y = \zeta(\sigma) \cdot y^n.$$

The map $\zeta : G_L \to \mathbf{C}_p$ thus defined is a continuous 1-cocycle for the group G_L. As $H^1(G_L, \mathbf{C}_p) = 0$ (as proved in [I-Z] Proposition 3.1) there exists an $\varepsilon \in \mathbf{C}_p$ such that $\zeta(\sigma) = \sigma(\varepsilon) - \varepsilon$ for all $\sigma \in G_L$. Now set $z_{n+1} := y - \varepsilon \cdot y^n$. This will do the job, as it is easy to see that $\sigma(y^n) = y^n$ for all $\sigma \in G_L$.

Before we prove ii) we need the following

Lemma 2.1. *Let L be a deeply ramified extension, $n \geq 1$ and $z \in (B_{n+1})^{G_L}$ a uniformizer and $y = \phi_n(z) \in (B_n)^{G_L}$. For each $a \in L[y]$ there exists $b \in L[z]$ such that $\phi_n(b) = a$ and if $n > 1$ then $w_{n+1}(b) \geq w_n(a) - 1$ and if $n = 1$ then $w_2(b) \geq v(a) - 2$.*

Proof. Let $\{\alpha_m\}_m, \alpha_m \in \bar{K}$ such that $\alpha_m \xrightarrow{w_{n+1}} z$. Then $\alpha_m \xrightarrow{w_n} y$.

Let now $a = \sum m_i y^i \in L[y]$, then $x_m := \sum m_i(\alpha_m)^i \xrightarrow{w_n} a$. Also $\{x_m\}_m$ is Cauchy in w_{n+1}, $x_m \xrightarrow{w_{n+1}} c := \sum m_i z^i \in L[z]$, and $\phi_n(c) = a$. Let us suppose $n > 1$. Then if $w_{n+1}(c) \geq w_n(a) - 1$ then we take $b = c$ and we are done. If not, we'll change c by an element of $z^n L = \mathrm{Ker}(\phi_n|_{L[z]})$, such that the desired inequality holds. First of all we may suppose that $w_n(a) = 0$ (if not we just multiply by a suitable power of p). Then $w_n(x_m) = 0$ for $m \gg 0$, so $x_m \in \mathcal{O}_{\bar{K}}^{(n-1)}$ for $m \gg 0$. Also as $\{x_m\}_m$ is a Cauchy sequence in w_{n+1}, we have $d_n(c) = d_n(x_m) \in \Omega^{(n)}$ for $m \gg 0$ as shown in section 1. We also have $\sigma(d_n(c)) = d_n(c)$ for all $\sigma \in G_L$, so $d_n(c) \in (\Omega^{(n)})^{G_L}$. As was explained in section 1, d_n extends to an $\mathcal{O}_{\mathbf{C}_p}[G_L]$-semilinear map, $d_n : J_{n+1} \to \Omega^{(n)}$, such that its restriction

$$(*) \qquad d_n : J_{n+1}^{G_L} \to (\Omega^{(n)})^{G_L}$$

is "almost surjective" (in the sense that its cokernel is annihilated by m_L.) Moreover, as in the proof of Theorem 2.2 i), $J_{n+1} \cong y^n \mathbf{C}_p$ as $\mathcal{O}_{\mathbf{C}_p}[G_L]$-modules. Therefore we have $J_{n+1}^{G_L} \cong y^n \hat{L}$, so from the almost surjectiveness of d_n in $(*)$, there exists $\beta \in z^n \hat{L}$ such that $pd_n(c) = pd_n(\beta)$. Moreover as $z^n L$ is dense in $z^n \hat{L}$ (in w_{n+1}), $\Omega^{(n)}$ is discrete and d_n is continuous, β can be chosen from $z^n L$. Finally we have $w_{n+1}(c - \beta) + 1 \geq 0 = w_n(a)$. So we take $b = c - \beta$ and we are done. The proof goes identically if $n = 1$, but $v(a)$ may not be made 0 by multiplying with a power of p, but $0 \leq v(a) < 1$.

Proof of the theorem. Let us denote by $z_n := \theta_n(z)$. It would be enough to prove that $L[z_n]$ is dense in $(B_n)^{G_L}$ for all $n \geq 1$. This statement is true for $n = 1$ as L is dense in $(\mathbf{C}_p)^{G_L}$. So let us suppose that it is true for some $n \geq 1$. Then we have the commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \to & (z_{n+1})^n \hat{L} & \to & (B_{n+1})^{G_L} & \xrightarrow{\phi_n} & (B_n)^{G_L} & \to & 0 \\
 & & \cup & & \cup & & \cup & & \\
0 & \to & (z_{n+1})^n L & \to & L[z_{n+1}] & \to & L[z_n] & \to & 0
\end{array}$$

The top exact sequence comes from considering the long exact cohomology sequence of the fundamental exact sequence above and the fact that $H^1(G_L, \mathbf{C}_p(n)) = 0$ ([I-Z] Proposition 3.1). The first vertical inclusion is dense in w_{n+1} and the third is dense in w_n. We want to prove that the middle inclusion is dense as well (in w_{n+1}).

Let $\alpha \in (B_{n+1})^{G_L}$ and let $a_i \in L[z_n]$ such that $a_i \xrightarrow{w_n} \phi_n(\alpha)$. We apply Lemma 2.1: there exist $c_i \in L[z_{n+1}]$, $i = 0, 1, 2, \ldots$ such that $\phi_n(c_0) = a_0$, $\phi_n(c_i) = a_{i+1} - a_i$, for $i > 0$ and $w_{n+1}(c_i) \geq w_n(a_{i+1} - a_i) - 2 \to \infty$. Therefore $c_i \xrightarrow{w_{n+1}} 0$. So let $b_i := c_0 + c_1 + \cdots + c_i \in L[z_{n+1}]$, then $\phi_n(b_i) = a_i$ and $\{b_i\}_i$ is Cauchy in w_{n+1}. Let $x \in B_{n+1}$ be the limit of $\{b_i\}_i$. Then, obviously $x \in (B_{n+1})^{G_L}$ and $\phi_n(x) = \phi_n(\alpha)$. Thus, $\alpha - x \in \mathrm{Ker}(\phi_n|_{(B_{n+1})^{G_L}}) = z^n \hat{L}$, say $\alpha - x = mz^n$, $m \in \hat{L}$. Let $s_i \in L$ be such that $s_i \xrightarrow{v} m$, then $s_i z^n \xrightarrow{w_{n+1}} mz^n$. So, $t_i := b_i + s_i z^n \in L[z_{n+1}]$ and $t_i \xrightarrow{w_{n+1}} \alpha$.

Remark 2.2. The same result was obtained by P. Colmez for the case where L is the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$ in [C], using different methods.

3. Generating elements

The main result of this section is the following rather surprising

Theorem 3.1. *There exists $z \in B_{dR}^+$ such that $\mathbf{Q}_p[\theta_n(z)]$ is dense in B_n for all $n \geq 1$ and $\mathbf{Q}_p[z]$ is dense in B_{dR}^+.*

Remark 3.1. For $n = 1$ this is an improvement of the result of [I-Z,1] where the authors proved that one can find an element z in $\mathbf{C}_p$ such that $\mathbf{Q}_p(z)$ is dense in $\mathbf{C}_p$.

Remark 3.2. Actually, Theorem 3.1 can be stated in an apparently stronger form: there exists $z \in B_{dR}^+$, such that $\mathbf{Q}[z]$ is dense in B_{dR}^+.

Before we start the proof of the theorem we need the following

Lemma 3.1 ("weak" Krasner's Lemma in B_n). *Let $n \geq 1$ be an integer, L any algebraic extension of $\mathbf{Q}_p$ and $\alpha, \beta \in \bar{\mathbf{Q}}_p$ such that*

$$w_n(\alpha - \beta) > \gamma_n(\alpha) := \max_{\sigma \in G_L, \sigma(\alpha) \neq \alpha} w_n(\alpha - \sigma(\alpha)).$$

Then $L(\alpha) \subset L(\beta)$.

Proof. If this were not true there would exist $\sigma \in \mathrm{Gal}(\bar{K}/L(\beta))$ such that $\sigma(\alpha) \neq \alpha$. Since $w_n(\alpha - \beta) = w_n(\sigma(\alpha - \beta)) = w_n(\sigma(\alpha) - \beta)$ and since w_n is a valuation we have

$$w_n(\alpha - \sigma(\alpha)) \geq w_n(\alpha - \beta)$$

which is a contradiction.

Remark 3.3. The "strong" Krasner's Lemma in B_n, which is left as an open problem, would be the same statement but for any β in B_n.

Proof of the theorem. We can find a sequence $\{a_n\}_{n\in\mathbf{N}}$ in $\bar{\mathbf{Q}}_p$ such that

$$\mathbf{Q}_p(a_1) \subset \mathbf{Q}_p(a_2) \subset \cdots \subset \mathbf{Q}_p(a_n) \subset \cdots \subset \bigcup_n \mathbf{Q}_p(a_n) = \bar{\mathbf{Q}}_p.$$

Now we construct a sequence of elements in $\bar{\mathbf{Q}}_p$, $\{\alpha_n\}_n$ together with a sequence of polynomials $\{h_{m,n}(X)\}_{(m<n)}$ in $\mathbf{Q}_p[X]$ having the following properties for each $n \in \mathbf{N}$:

i) $h_{m,n}(\alpha_n) = \alpha_m$ for any $m < n$.

ii) $\bigcup \mathbf{Q}_p(\alpha_n) = \bar{\mathbf{Q}}_p$.

iii) $w_n(\alpha_n - \alpha_{n+1}) > \max\{n, \gamma_n(\alpha_n), \delta_n\}$, where γ_n was defined in Lemma 3.1 and

$$\delta_n := \max_{m_1<m_2\le n}\ \max_{1\le j\le \deg(h_{m_1,m_2})} \frac{n - w_n(h^{(j)}_{m_1,m_2}(\alpha_n)) + w_n(j!)}{j}$$

(here, if $h \in \mathbf{Q}_p[X]$ and j is a nonnegative integer then we denote by $h^{(j)}$ the j-th derivative of h.)

The construction goes like in [I-Z,1], namely we choose our sequence $\{\alpha_n\}_n$ to have also the property

iv) $\mathbf{Q}_p(a_n) \subset \mathbf{Q}_p(\alpha_n)$.

First we take $\alpha_1 := a_1$. Suppose we have constructed $\alpha_1, \alpha_2, \dots \alpha_n$ and $h_{i,j}(X)$ for $i < j \le n$ and we want to find α_{n+1} and $h_{m,n+1}(X)$ for $m \le n$. We take (as in [I-Z,1]) α_{n+1} of the form $\alpha_{n+1} = \alpha_n + t_n \cdot a_{n+1}$, where $t_n \in \mathbf{Q}_p$ is "small" enough to have iii) above. From Lemma 3.1 it follows that $\mathbf{Q}_p(\alpha_n) \subset \mathbf{Q}_p(\alpha_{n+1})$, so $a_{n+1} = \frac{1}{t_n}(\alpha_{n+1} - \alpha_n) \in \mathbf{Q}_p(\alpha_{n+1})$, i.e. we have iv) for α_{n+1}. This will imply property ii) after the construction is done. Also, from the fact that $\mathbf{Q}_p(\alpha_n) \subset \mathbf{Q}_p(\alpha_{n+1})$ it follows the existence of $h_{n,n+1}(X)$ satisfying the required property. We define simply

$$h_{m,n+1}(X) := h_{m,n}(h_{n,n+1}(X)) \qquad \text{for } m < n.$$

Hence the inductive procedure works, and so we have a sequence $\{\alpha_m\}_m$, which is Cauchy in w_n, for all $n \ge 1$, and also Cauchy in B_{dR}^+. Let us denote by $z_n \in B_n$ and by $z \in B_{dR}^+$, the elements with the property: $\alpha_m \xrightarrow{w_n} z_n$ for all $n \ge 1$, and $\lim_m \alpha_m = z$ in B_{dR}^+. Hence $z_n = \theta_n(z)$ for all $n \ge 1$. We'd like to show that $\mathbf{Q}_p[z_n]$ is dense in B_n for all $n \ge 1$ and $\mathbf{Q}_p[z]$ is dense in B_{dR}^+. For this it would be enough to show that $\bar{\mathbf{Q}}_p$ is contained in the topological closure of $\mathbf{Q}_p[z_n]$ in B_n for all n and in the topological closure of $\mathbf{Q}_p[z]$ in B_{dR}^+. We'll show that for a fixed but arbitrary r, α_n is in the topological closure of $\mathbf{Q}_p[z_r]$ in B_r, for all n.

So let us fix two arbitrary positive integers r and m_1. We also fix m_2 such that $m_2 > m_1$ and $m_2 > r$ and $n \ge m_2$. Let us denote by $u_n := \alpha_{n+1} - \alpha_n$. We have

$$w_r(h_{m_1,m_2}(\alpha_n) - h_{m_1,m_2}(\alpha_{n+1})) \ge w_n\left(\sum_{j\ge 1} h^{(j)}_{m_1,m_2}(\alpha_n)\cdot \frac{u_n^j}{j!}\right)$$

$$\ge \min_{1\le j\le \deg(h_{m_1,m_2})} (j w_n(u_n) + w_n(h^{(j)}_{m_1,m_2}(\alpha_n)) - w_n(j!))$$

where the first inequality comes from the Taylor expansion of $h_{m_1,m_2}(\alpha_{n+1})$ and the property d) of the w_n's. Since $w_n(u_n) > \delta_n$ we get from iii) the following relation

$$\text{v)} \qquad w_r(h_{m_1,m_2}(\alpha_n) - h_{m_1,m_2}(\alpha_{n+1})) \geq n.$$

Let now $m_3 > m_2$. From v) above we get

$$w_r(h_{m_1,m_2}(\alpha_{m_2}) - h_{m_1,m_2}(\alpha_{m_3})) = w_r\left(\sum_{n=m_2}^{m_3-1}(h_{m_1,m_2}(\alpha_n) - h_{m_1,m_2}(\alpha_{n+1}))\right)$$

$$\geq \min_{m_2 \leq n \leq m_3} w_r(h_{m_1,m_2}(\alpha_n) - h_{m_1,m_2}(\alpha_{n+1})) \geq m_2.$$

Now we let m_3 go to infinity and deduce from the fact that $h_{m_1,m_2}(\alpha_{m_3}) \xrightarrow{w_r} h_{m_1,m_2}(z_r)$ and $h_{m_1,m_2}(\alpha_{m_2}) = \alpha_{m_1}$ for all m_2 that

$$w_r(\alpha_{m_1} - h_{m_1,m_2}(z_r)) \geq m_2.$$

Therefore we see that we can approximate α_{m_1}, in the valuation w_r, as well as we want with polynomials $h_{m_1,m_2}(z_r) \in \mathbf{Q}_p[z_r]$. Thus the topological closure of $\mathbf{Q}_p[z_r]$ in B_r contains all the α_n, so it contains all the fields $\mathbf{Q}_p(\alpha_n) = \mathbf{Q}_p[\alpha_n]$ so it contains $\bar{\mathbf{Q}}_p$ and hence it equals B_r. This finishes the proof.

Now that we have constructed generating elements z in B_{dR}^+ one naturally might wonder if these elements could be also used to generate the modules of differential forms (see section 1). Let us fix some integer $n \geq 2$ then as shown in [I-Z], $d^{(n-1)}$ induces an $\mathcal{O}_{\bar{\mathbf{Q}}_p}$-linear homomorphism $d^{(n-1)} : J_n \to \Omega^{(n-1)}$, which is continuous with respect to w_n on J_n and the discrete topology on $\Omega^{(n-1)}$ and surjective. Therefore if $z \in B_{dR}^+$ is a "generating element" then any element in $\Omega^{(n-1)}$ will have the form $d^{(n-1)}(P(\theta_n(z)))$ for some polynomial $P(X)$ with coefficients in $\mathbf{Q}_p$. This doesn't mean, however, that $d^{(n-1)}(z)$ generates $\Omega^{(n-1)}$ as an $\mathcal{O}_{\bar{K}}$ module. Actually we know that this is impossible since $\Omega^{(n-1)}$ is p-divisible. What happens is that the coefficients in the above polynomials $P(X)$ have larger and larger powers of p in their denominators. Therefore if one wants to generate $\Omega^{(n-1)}$ in terms of $\theta_n(z)$ one needs to use a sequence of polynomials in $\theta_n(z)$ such that no finite power of p will annihilate all their differentials.

4. An orthonormal basis for B_n

Let us fix an $n \geq 1$ and a "generating element" $z \in B_n$ over $\mathbf{Q}_p$ (we recall that such an element has the property that $\mathbf{Q}_p[z]$ is dense in B_n). Such an element exists by Theorem 3.1, and actually can be chosen such that $\eta_n(z)$ is a "generating element" of $\mathbf{C}_p$. Moreover we may suppose that $w_n(z) > 0$ (if not we just multiply z by a suitable power of p). For any $m \geq 1$ we define

$$\delta(m, z) := \sup\{w_n(f(z)) \mid f \in \mathbf{Q}_p[X], \text{ monic}, \deg f \leq m\}.$$

We have

Lemma 4.1. *$\delta(m, z)$ is an integer for all m.*

Proof. It would be enough to show that $\delta(m, z)$ is finite. Suppose not, then from the inequality $w_n(f(z)) \le v(f(\eta_n(z)))$ we deduce that

$$\sup\{v(f(\eta_n(z))) \mid f \in \mathbf{Q}_p[X],\ \text{monic},\ \deg f \le m\} = \infty.$$

As $\mathbf{Q}_p$ is locally compact, there exists a Cauchy sequence of polynomials of degree at most m, $\{f_k(X)\}_{k \in \mathbf{N}}$, such that $v(f_k(\eta_n(z))) \to \infty$ as $k \to \infty$. The $\mathbf{Q}_p$-vector space of polynomials of degree at most m is complete so let us denote by $f(X) := \lim_{k\to\infty} f_k(X)$. Then $f(\eta_n(z)) = 0$ and so $\eta_n(z)$ is algebraic of degree at most m over $\mathbf{Q}_p$. This contradicts the fact that $\eta_n(z)$ is a generating element of $\mathbf{C}_p$.

For each $m \ge 1$ let us choose $f_m \in \mathbf{Q}_p[X]$ monic of degree at most m such that

$$\delta(m, z) = w_n(f_m(z)).$$

We'll call the polynomials f_m "admissible". We have the following

Lemma 4.2. $\deg(f_m) = m$.

Proof. The proof follows easily from the fact that

$$\delta(m+1, z) > \delta(m, z), \qquad \text{for all } m$$

This relation follows from the more general inequality: for all $m_1, m_2 \ge 0$ we have $\delta(m_1 + m_2, z) \ge \delta(m_1, z) + \delta(m_2, z)$ and the fact that $\delta(1, z) \ge w_n(z) > 0$.

In order to prove this formula let us see that

$$w_n(f_{m_1+m_2}(z)) \ge w_n(f_{m_1}(z) \cdot f_{m_2}(z)) \ge w_n(f_{m_1}(z)) + w_n(f_{m_2}(z)).$$

Let now $\{f_m(X)\}_m$ be a sequence of "admissible" polynomials, and for each $m \ge 1$ we define $r_m := w_n(f_m(z))$ and $M_m(z) := f_m(z)/p^{r_m}$. We set $M_0(z) := 1$. Then we have

Corollary 4.1. *If $m_0 \ge 1$ then $\{M_0, M_1, \dots, M_{m_0}\}$ is a basis for the $\mathbf{Q}_p$-vector space of polynomials of degree less than or equal to m_0 with coefficients in $\mathbf{Q}_p$.*

The main result of this section is

Theorem 4.1. *$\{M_m(z)\}_{m\ge 0}$ is an integral, orthonormal basis of B_n, as a Banach space over $\mathbf{Q}_p$. More precisely:*

i) *For any $y \in B_n$ there exists a unique sequence $\{c_m\}_{m\ge 0}$ in $\mathbf{Q}_p$ such that $c_m \xrightarrow{v} 0$ and $y = \sum_m c_m M_m(z)$.*

ii) *Let $y \in B_n$, $y = \sum_m c_m M_m(z)$, with $c_m \in \mathbf{Q}_p$ for all $m \ge 0$ and $c_m \xrightarrow{v} 0$. Then $w_n(y) = \min_m v(c_m)$.*

iii) *For all $y \in B_n$, $w_n(y) \ge 0$ if and only if $y = \sum_m c_m M_m(z)$ with $c_m \in \mathbf{Z}_p$ for all $m \ge 0$ and $c_m \xrightarrow{v} 0$.*

Proof. Property iii) obviously follows from i) and ii). Let us first prove ii). For this let us consider a finite sum: $y = \sum_{m=0}^{N} c_m M_m(z)$, with $c_m \in \mathbf{Q}_p$ for all m. Let m_0 be the largest index k such that $\min\{v(c_m)\} = v(c_k)$. We claim that:

$$w_n\left(\sum_{m=1}^{m_0} c_m M_m(z)\right) = v(c_{m_0}).$$

Obviously we have that the right hand side is less than or equal to the left hand side. Let us suppose that the inequality is strict. Then we have

$$w_n\left(\sum_{m=1}^{m_0} \frac{p^{r_{m_0}}}{c_{m_0}} c_m M_m(z)\right) > r_{m_0} = \delta(m_0, z).$$

But, $\sum_{m=0}^{m_0} \frac{p^{r_{m_0}}}{c_{m_0}} c_m M_m(z)$ is a monic polynomial of degree m_0 in z, so the above inequality contradicts the definition of $\delta(m_0, z)$. So the claim follows. On the other hand one has

$$w_n\left(\sum_{m=m_0+1}^{N} c_m M_m(z)\right) > v(c_{m_0})$$

so

$$w_n\left(\sum_{m=1}^{N} c_m M_m(z)\right) = v(c_{m_0}).$$

Therefore ii) holds true for finite sums, so also for sums of the form $\sum_{m\geq 0} c_m M_m(z)$, where $c_m \overset{v}{\to} 0$. Thus ii) is proved.

Now let us prove i). Let $y \in B_n$ and as z is a "generating element", we have a sequence of polynomials $P_m(X) \in \mathbf{Q}_p[X]$, such that

$$P_m(z) \overset{w_n}{\to} y.$$

Let $k_m := \deg(P_m(X))$. By Corollary 4.1 each $P_m(z)$ can be written $P_m(z) = \sum_{j=0}^{k_m} c_{m,j} M_j(z)$ such that $w_n(P_m(z)) = \min_j v(c_{m,j})$ from the above discussion. As the sequence $\{P_m(z)\}_m$ is Cauchy in w_n, for each j, the sequence $\{c_{m,j}\}_m$ is Cauchy in v (as $w_n|_{\mathbf{Q}_p} = v$), so let us define $c_j := \lim_m c_{m,j} \in \mathbf{Q}_p$. Moreover we claim that $v(c_j) \to \infty$. To see this let us fix $\varepsilon > 0$ and fix also m_ε such that $w_n(P_{m_\varepsilon}(z) - y) > \frac{1}{\varepsilon}$. For all $j > \max(m_\varepsilon, k_{m_\varepsilon})$ fixed, let m be big enough such that $w_n(P_m(z) - P_{m_\varepsilon}(z)) > \frac{1}{\varepsilon}$, so we have $v(c_{m,j} - c_{m_\varepsilon,j}) > \frac{1}{\varepsilon}$. So we get (letting m go to infinity) $v(c_j - c_{m_\varepsilon,j}) > \frac{1}{\varepsilon}$ and $c_{m_\varepsilon,j} = 0$ as $j > k_{m_\varepsilon}$. This proves the claim. So it now makes sense to consider

$$\tilde{y} := \sum_{m=0}^{\infty} c_m M_m(z) \in B_n.$$

From the construction of $\tilde{y}$ we have $P_m(z) \overset{w_n}{\to} \tilde{y}$, so $\tilde{y} = y$. The uniqueness statement of i) follows easily from ii).

Remark 4.1. If in Theorem 4.1 we consider z as a "generating element" of B_n over K (let us recall that $K = \mathbf{Q}_p^{ur}$) then the same construction gives an integral, orthonormal basis of B_n over $\hat{K}$.

5. Metric invariants for elements in B_{dR}^{+}

Although the topology in B_{dR}^{+} does not come from a canonical metric, the B_n's do have canonical metric structures. This shows us a way to obtain metric invariants for elements in B_{dR}^{+}, by sending them canonically to any B_n and recovering various metric invariants from those metric spaces.

For example, one may consider for any Z in B_{dR}^{+} the invariants $\delta_n(m, Z) := \delta(m, (\theta_n(Z)))$.

We mention that at level $n = 1$ (i.e. in $\mathbf{C}_p$) one knows a lot more about these admissible sequences than we presently know in B_n, for $n > 1$, or in B_{dR}^{+}. More details can be found in [P-Z] and [A-P-Z]. Can any of those results be obtained at higher levels or in B_{dR}^{+}?

In [A-P-Z] it is proved that one can separate the conjugates of Z from the nonconjugates using certain metric invariants. Let us recall how this is done: for any Z in $\mathbf{C}_p - \bar{\mathbf{Q}}_p$ the sequence $\{\delta(m, Z)/m\}_m$ has a limit $l(Z)$ in $\mathbf{R} \cup \{\infty\}$. Now we take a "distinguished" sequence $f_m(X)$ for Z (this is canonically a subsequence of what we called in this paper an "admissible" sequence of polynomials for Z, see [A-P-Z]) and define for any y in $\mathbf{C}_p$, $l(y, Z) := \lim_m \sup v(f_m(y))/m$. Then $l(y, Z) \leq l(Z)$ for any y in $\mathbf{C}_p$ and this holds with equality if and only if y and Z are conjugate. This provides us with a metric characterization for the set of conjugates of Z, as the set of zeros of the function $f(y) = l(Z) - l(y, Z)$. What will be the analogous result at higher levels or in B_{dR}^{+}?

From the proof of Lemma 4.2 it follows easily that for any z in B_n the sequence $\{\delta(m, z))/m\}_m$ has a limit, say $l(z)$. Now if Z is in B_{dR}^{+} we get a sequence of metric invariants for Z, given by $l_n(Z) := l(\theta_n(Z))$. What can be said about this sequence?

Since w_n is dominated by w_{n-1} it is clear that $\delta(m, \theta_n(Z)) \leq \delta(m, \theta_{n-1}(Z))$ for any m, n and Z. Therefore one has: $l_1(Z) \geq l_2(Z) \geq \cdots \geq l_n(Z) \geq \cdots$

The questions concerning metric characterizations for the set of conjugates is particularly interesting for generating elements, for the following reason: If we define for any Z in B_{dR}^{+} (or in some B_n) $C(Z) := \{\sigma(Z) \mid \sigma \in G\}$, where as always $G := \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ we have a continuous surjective map from G to $C(Z)$ given by $\sigma \to \sigma(Z)$. Now if Z is a generating element in B_{dR}^{+} (or in B_n respectively) then the above map is one-to-one and moreover it is a homeomorphism. So one can view G as lying inside B_{dR}^{+} via the orbits $C(Z)$ of these generating elements.

Another class of invariants can be obtained in the following way. We take an admissible sequence of polynomials $\{f_m(X)\}_m$ for an element $z \in B_n$ and consider the sequence $\{w_n(f'_m(z))\}_m$. In the definition of admissible sequences the derivatives $f'_m(X)$ played no role and so we have no reason to expect that the numbers $w_n(f'_m(z))$ are independent of the admissible sequence considered. The following result might then come as a surprise.

Proposition 5.1. *Let z be a "generating element" of B_n, for some $n \geq 1$. There is an infinite subset $\mathcal{M} = \mathcal{M}(z)$ of* $\mathbf{N}$ *such that the sequence $\{w_n(f'_m(z))\}_{m \in \mathcal{M}}$ is independent of the particular admissible sequence $\{f_m(X)\}_m$ considered.*

Remark 5.1. If Z is a generating element of B_{dR}^+ then for any n we get a sequence of invariants for Z, namely:

$$\delta'_n(m, Z) := w_n(f'_m(\theta_n(Z)) \qquad m \in \mathcal{M}(\theta_n(Z)).$$

Here the sets $\mathcal{M}(\theta_n(Z))$ might be different for different n's.

Proof. Let us fix an admissible sequence $\{f_m(X)\}_m$ for z. We claim that the sequence $\{b_m\}_m$ defined by

$$b_m := w_n(f'_m(z)) - w_n(f_m(z)) \qquad \text{for all } m$$

is not bounded from below. Suppose not, and let $b \in \mathbf{Z}$ be a lower bound for the sequence $\{b_m\}_m$. Let us first observe that the b_m's are unchanged if we replace in their definition the $f_m(X)$'s by the $M_m(X)$'s (the M_m's are defined in section 4). So we have

$$w_n(M'_m(z)) = b_m \geq b \qquad \text{for all } m.$$

Then the derivative with respect to z gives us a $\mathbf{Q}_p$-linear operator

$$\frac{\partial}{\partial z} : \mathbf{Q}_p[z] \to \mathbf{Q}_p[z]$$

which is continuous since it is bounded on the orthonormal basis $\{M_m(z)\}_m$ by the assumption. Since $\mathbf{Q}_p[z]$ is dense in B_n, the operator $\frac{\partial}{\partial z}$ has a unique extension to a continuous, $\mathbf{Q}_p$-linear operator $\Psi : B_n \to B_n$. Clearly Ψ is a derivation of B_n, which is trivial on $\mathbf{Q}_p$. We now look at its restriction to $\bar{\mathbf{Q}}_p$. If $\alpha \in \bar{\mathbf{Q}}_p$ and $P_\alpha(X)$ is its minimal polynomial over $\mathbf{Q}_p$, then we have:

$$0 = \Psi(P_\alpha(\alpha)) = P'_\alpha(\alpha)\Psi(\alpha).$$

Since $P'_\alpha(\alpha) \neq 0$ it follows that $\Psi(\alpha) = 0$. So Ψ is trivial on $\bar{\mathbf{Q}}_p$ and by continuity it is trivial on B_n. But this is a contradiction with the fact that $\frac{\partial}{\partial z}$ is non-trivial on $\mathbf{Q}_p[z]$. This proves the claim. Now let $\mathcal{M}$ be the infinite set of those indices m for which we have:

$$\min\{b_j \mid 0 \leq j \leq m-1\} > b_m.$$

Our second claim is that for any other admissible sequence of polynomials $\{g_m(X)\}_m$ for z, we have

$$w_n(g'_m(z)) = w_n(f'_m(z)) \qquad \text{for all } m \in \mathcal{M}.$$

In order to prove our second claim, let us denote by $\{G_m(z)\}_m$ the orthonormal basis of B_n over $\mathbf{Q}_p$ obtained from $\{g_m(X)\}_m$. Let $m_0 \in \mathcal{M}$. Since

$$\frac{g_{m_0}(X)}{G_{m_0}(X)} = \frac{f_{m_0}(X)}{M_{m_0}(X)}$$

we are done if we prove that $w_n(G'_{m_0}(z)) = w_n(M'_{m_0}(z))$. At this point we use the basis $\{M_m(z)\}_m$ to write

$$G_{m_0}(z) = \sum_{j=0}^{m_0} c_j M_j(z)$$

with $c_j \in \mathbf{Q}_p$. As $w_n(G_{m_0}(z)) = 0$ (by the construction of the G_m's) we get from Theorem 4.1 iii) that $c_j \in \mathbf{Z}_p$ for all $0 \le j \le m_0$. Moreover looking at the leading coefficients of G_{m_0} and M_j we get that $c_{m_0} = 1$. We have

$$G'_{m_0}(z) = \sum_{j=1}^{m_0} c_j M'_j(z).$$

Now for any $j < m_0$ we have

$$w_n(c_j M'_j(z)) = v(c_j) + w_n(M'_j(z)) \ge w_n(M'_j(z)) = b_j > b_{m_0} = w_n(M'_{m_0}(z)).$$

Therefore

$$w_n(G'_{m_0}(z)) = w_n(M'_{m_0}(z)).$$

This proves the Proposition.

CICMA (McGill University and Concordia University),
Department of Mathematics,
805 Sherbrooke West, Montreal,
QC, Canada, H3A 2K6
e-mail: iovita@scylla.math.mcgill.ca

Institute of Mathematics of the Romanian Academy,
P.O. Box 1-764,
70700 Bucharest, Romania

Massachusetts Institute of Technology,
Department of Mathematics,
77 Mass. Avenue, Cambridge,
MA 02139, USA.
e-mail: azah@math.mit.edu

References

[A-P-Z] V. Alexandru, N. Popescu and A. Zaharescu, On the closed subfields of $\mathbf{C}_p$, Journal of Number Theory, **68**-2 (1998), 131–150.

[C] P. Colmez, Théorie d'Iwasawa des Représentations de de Rham d'un corps local, preprint, 1996.

[C-G] J. Coates and R. Greenberg, Kummer Theory of Abelian Varieties, Invent. Math., **126**, no 1–3 (1996), 129–174.

[Fo] J.-M. Fontaine, Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate, Ann. of Math., **115** (1982), 529–577.

[F-C] J.-M. Fontaine, Le corps des Périodes p-Adiques (avec une appendice par P. Colmez), Astérisque **223** (1994).

[I-Z,1] A. Iovita and A. Zaharescu, Completions of r.a.t-Valued fields of Rational Functions, Journal of Number Theory, **50**-2 (1995), 202–205.

[I-Z] A. Iovita and A. Zaharescu, Galois theory of B_{dR}^{+} to appear in Compositio Mathematica.

[P-Z] N. Popescu and A. Zaharescu, On the Structure of Irreducible Polynomials Over Local Fields, Journal of Number Theory, **52**-1 (1995), 98–118.